How hard can it be?

What you need to know about integrating biometrics

Catherine J. Tilton

Director, Special Projects, SAFLINK

11417 Sunset Hills Rd, Suite 106
Reston, VA 20190
703-708-9280
(fax) 703-708-0014
ctilton@saflinkcom

Agenda

- Introduction
- Requirements
- Alternative evaluation
- Biometric system design
- Infrastructure integration
- Conclusion

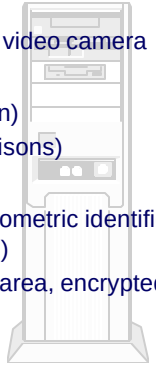
Introduction

- Will address
  - Unique considerations and guidelines for integrating biometrics into new or existing systems
- Will not address
  - Basics of biometrics
  - Project management 101
  - Aspects common to any system development

Biometric Requirements

Requirements

- What do I need to make it work?
  - Capture device
    - Finger scanner, microphone, video camera
  - Algorithms
    - Processing (feature extraction)
    - Matching (1:1 or 1:N comparisons)
  - Repository
    - Database to store enrolled biometric identifier records (for later comparison)
    - Should be protected (secure area, encrypted)



Requirements Definition

- #1 - first define the problem you are trying to solve
  - results you are trying to achieve
- Requirement come in various forms and sources
  - Tasking from management, other departments, marketing
  - Customer solicitation
  - May need to be elicited
- Requirements state WHAT not HOW

Customer service

Audit

Security

Deter theft

Reduce fraud

Terrorist surveillance

Convenience

Track inmates

Find missing children

Speed processing

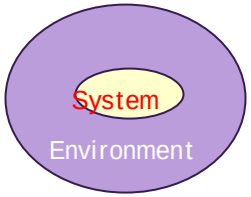
Requirements Definition

- Types of requirements
  - Physical (size, weight, material)
  - Functional (must do this, that)
  - Performance (how fast, how accurate)
  - Quality (reliability, workmanship, supportability)
- Good requirements
  - Clear, concise -- Written down, tracked
  - Unambiguous -- Agreed to by accepter
  - Testable (verifiable)

How do you know when you're done?

Requirements Definition

- Identify constraints
  - Environment
  - Interfaces
  - Legacy systems
  - Budget (initial + life cycle)
  - Standards
  - Physical
  - Personnel
  - Political/social/cultural/legal



Biometric Requirement Considerations

- Accuracy (FAR/FRR trade-off)
- Poor candidates/poor enrollments
- Interference sources
- Scalability
- DB size
- Response time
- Simultaneous requests
- Data protection/encryption
- Save or pitch raw data?
- Multiple biometrics?
- Interoperability/interchange
- Deployment considerations
  - Indoor/outdoor
  - Geographically dispersed (remote enrollment?)
- How tell if system working
- Use of standards
- Privacy issues
- Training
- Platform considerations
- Device issues
- Human factors

Biometric Requirements

- Know your
  - User population
  - Environment
  - Application
- Address the exception cases
  - How do I handle
    - A false reject?
    - A poor enrollment?
    - How do I detect a false accept?
  - What do I do with a subject with a poor biometric?
  - What happens if the device fails?
  - What if the person's biometric is temporarily unavailable (injury, laryngitis, etc.)

Risk Management

- Identify, address, and reduce/eliminate sources of risk before they threaten success
- Risk identification
  - List potential risks
- Risk Analysis
  - Assess likelihood of risks
  - Assess impact if realized
- Risk Control
  - Develop risk prevention & mitigation strategies
  - Monitor risk factors

Biometric Project Risks

- Technology impacted by user behavior and environment
- System components new and unproven
- User perceptions can have unexpected impact
- Unrealistic expectations by stake holders
- Enrollment logistics
- Response times
- Vague requirements
- Patchwork integration

- PLUS - all normal system development project risks

Biometric Planning Considerations

- Education/awareness campaign prior to roll out
  - Perception dependent on how technology is introduced
- Have privacy policy in place in advance
- Need whole solution, not just hardware and software
- Early testing
- Set expectations
- Know target environment
- Agreement from customer on requirements/design
- Enrollment plan

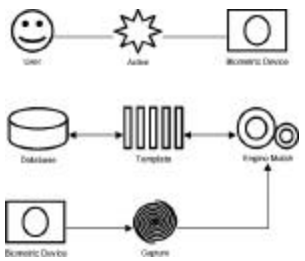
Privacy considerations

- IBIA privacy principles (www.ibia.org)
- Privacy blueprint *
  - ***Notice*** - no clandestine capture or secret databases
  - ***Access*** - subject right to find out if his biometric data is in the database and how it is being used
  - ***Correction Mechanism*** - ability to correct or make changes to biometric data
  - ***Informed Consent*** - knowingly provided; provided for specific purpose; no 3rd party disclosure w/o consent
  - ***Reliability & Safeguarding*** - protect integrity and confidentiality (adequate precautions)

* John Woodward, "Private Sector Use of Biometrics: The Need to Safeguard Privacy Concerns -- The Need for a Biometric Blueprint"

Biometric Design Model

- BANTAM
  - Biometric and Token Application Modeling Tool
  - Julian Ashbourn (AVANTI fame)
- Provides specific notation for biometric systems



Identify and Evaluate Alternative Solutions

Evaluation Process

- To meet requirements, consider biometric and non-biometric solutions
- If biometrics are selected, evaluate:
  - Which biometric type or combination of types
    - If multiple biometrics, singular or layered
    - Use in combination with other technologies?
  - 1:1 or 1:N solution
  - Type/setting of threshold
  - Model adaptation

Consider Alternatives to Biometrics

- Identification numbers or aliases
- Long term secrets
  - "Mother's Maiden Name"
  - Passwords
- Identification cards/badges
  - Descriptive information (biometric?)
  - Signature
  - Photograph
- Smart Cards/RF cards/Prox cards/Tokens
- Challenge/Response systems
- Digital Certificates
- Security guards
- Keys

Reasons to Choose Biometrics

- Biometrics link the event to a particular individual, not just to a password or token, which may be used by someone other than the authorized user
- Convenient - nothing to carry or remember
- Inexpensive
- Accurate - positive authentication
- Prevents impersonation
  - Protects against identity theft
- Strong authentication
  - System/network access, encryption keys, digital certificates
- Protects privacy
- Provides audit trail
- Degree of nonrepudiation

Selection of Biometric Technology

- Several viable technologies
  - Fingerprint
  - Hand/finger geometry
  - Voice
  - Face
  - Iris
  - Signature
- Evaluation criteria
  - Price
  - Performance
  - Project goals and requirements

Evaluation Criteria

Match technology to requirements

- User/Environment considerations
  - Cooperative/non-cooperative users
  - Overt/covert capture
  - Habituated/non-habituated
  - Attended/unattended
  - Public/private
  - Indoor/outdoor
  - Possible interference
  - User lifestyle/occupation
  - Compatibility with existing/legacy systems
- Technology factors
  - Cost
  - Accuracy
  - Ease of use
  - Public acceptance
  - Long term stability
  - Existence/use of standards
  - Barriers to attack
  - Track record of vendor/product
  - Availability of alternate sources
  - Scalability

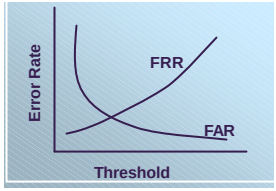
Comparison

	Iris	Face	Finger	Signature	Voice
Accuracy	Very High	High	High	High	High
Ease of Use	Medium	Medium	High	High	High
Barrier to Attack	Very High	Medium	High	Medium	Medium
Public Acceptance	Medium	Medium	Medium	Very High	High
Long Term Stability	High	Medium	High	Medium	Medium
Potential Interference	Poor Lighting	Lighting Aging, Glasses, Hair	Dryness Dirt, Age, Race	Changing Signatures	Noise, Colds, Weather

Source: ICSA

Accuracy

- False Accept Rate(FAR)
  - False Match
- False Reject Rate (FRR)
  - False Non-match
- Equal Error Rate (EER)
- Failure to Enroll (FTE)



Barriers to Attack

- Threat Analysis
  - Access risk in the context of the complete security solution
- Trust Model
  - Where are the trusted system boundaries
- Public perceptions
- Cooperation of user
- Reality check -- All systems are susceptible to attack ala “Mission Impossible”
- Safe analogy

Long-Term Stability

- Does the physical or behavioral characteristic change over time?
- Impacts System Design
  - Biometric that evolves over time requires constant and automatic “improvement” of template
    - Dynamic signature, voice, face
    - Adaptation, training

Testing & Certification

- How do you validate vendor claims?
  - Vendor test results
    - Generally performed under lab conditions
  - Internal (self) testing
    - Tests within close to actual environment/real users
    - Can do in lab, as part of eval, or as pilot
    - Requires internal expertise and adequate subjects
  - 3rd party testing (commissioned or test reports)
    - NPL/CESG, NIST, BMO, etc.
    - IBG, SJSU, ICSA, Security Labs
- What do you test for?
  - Accuracy, response time, reliability
  - Ease of use/installation/administration, suitability for purpose
  - Security/assurance
  - Standards compliance

Multiple Biometrics

- Biometrics can be used to replace or augment other authentication mechanisms
  - Biometric + token; biometric + password
- Multiple biometrics
  - Singular use
    - Authentication: Different biometrics for different users or settings
    - Improve performance because of better match of environment or user
  - Layered (combined) use
    - Authentication: Pass all tests or dynamic voting/weighting schemes
    - Improve performance with complementing biometric technology

Biometrics and Smart Cards

- Biometrics sometimes seen as competitor to smart cards and sometimes as complimentary
- When used together -
  - Biometrics may be used as a 2nd factor for authentication (token + biometric must be present)
  - Biometrics can be used to access/activate the card
  - Biometrics can be used to unlock secrets on the smart card (e.g., private key, dig certif, PIN, etc.)
  - The biometric template can be stored on the card, with authentication of the individual against the info on the card
  - Ensures user is legitimate holder of card

Biometrics and Smart Cards

- Comparison when competing -
  - Smart cards require distribution & inventory control
    - Lost/stolen cards, re-issue, revocation
    - Replacement cost
  - Generally requires use of PW or PIN in conjunction with card
  - Tokens not tightly bound to individual
    - Shared with bosses, colleagues, secretaries
    - Left in unlocked desk drawers
    - No non-repudiation
  - Costs:
    - Similar HW costs (depending on biometric selected)
      - Card reader vs fingerprint reader/camera/mic
    - Similar procurement costs; biometrics lower operating cost
  - Both beginning to be available in standard peripherals
  - Industry standards evolving for both

Biometrics and PKI

- Sometimes seen as competing technologies
- Can be complementary
- PKI totally dependent upon protection of the private key
  - Confidentiality, integrity, access control
- Passwords and PINs are inadequate for this purpose
- Biometrics can provide the means of strong authentication needed to 'release' the private key for use
- Conversely, PKI/encryption can be used to protect the biometric data during transmission & storage

INFOSEC Requirements

	PKI	Biometrics
I&A	PW based	Unique
Authorization	Supports	Supports
Integrity	Dig Cert	No
Confidentiality	Encryption	No
Non-repudiation	In doubt	Yes
Detection	No	No

Strength in Combination

Mutual Benefits

USES ▲ ▶

	Biometrics	Smart Cards	PKI
Biometrics		• SC portable/secure template storage • User ID • 2nd authen. Factor • SC becomes BSP	• Secure template during xmt/store • Dig sign template • Dig sign components
Smart Cards	• Access ctrl to card • Unlock secrets on card • Verify cardholder as cardowner		• Secure data on card • Secure reader I/F • Mut auth. SC apps.
PKI	• Protect access to private key/dig cert. • Enhance non-repudiation	• SC becomes CSP • SC portable/secure key/cert storage	

1:1 -vs- 1:N

Biometric Authentication:

1:1 Match

- Requires declared identity
- Convenient - in a keyboard/card
- Accurate
- Inexpensive
- Applications
  - System/network access, Password/PIN replacement, Physical access control

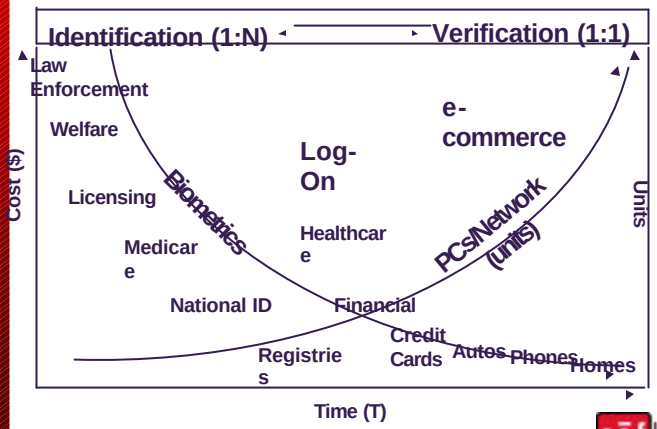
Biometric Identification:

1:N Match

- Finds duplicates
- Exposes fraud or criminal activity
- Requires human analysis
- Expensive
- Applications
  - Law enforcement, National ID, Voter registration, Driver's license, Welfare . . .

1: Few: Finds match in small number (<500) of records, sequence of 1:1 matching.

Application Trade-Offs



1:N Considerations

- Database size (scalability - up/down)
- Accuracy
- Response times
- Binning, filtering, preselection
- Additional template parameters to speed search
- FP - pattern classification, subpattern classification
- Communication bandwidth
- Output - candidate list
- Manual review / intervention
- Error sources (capture quality, FE, binning, matching)
- Modeling & simulation (peak load)

Threshold Comparison

- Biometric Algorithms return a measure of similarity in a match or confidence value. A threshold is established to indicate a match.
- Default Threshold - Same value used through out system
- Individual Threshold - Threshold value assigned to user based on attributes of enrollment
- Dynamic Threshold - Threshold is adjusted dynamically based on a variety of factors
  - Security level, Environment, Transaction amount, etc ...

Adaptation

- Model/template adaptation
  - Upon a successful match, the biometric technology module/engine may return an updated template
  - Generally combines old + new data
  - Keeps registered enrollment data “fresh”
  - Accommodates change in measured characteristic over time
  - Examples:
    - Aging of face/voice
    - Changes in writing style

Biometric System Design

Biometric System Design

- Enrollment
- Verification
- Architecture
  - Storage/matching locations
  - Components
  - Security
  - Ancillary functions
  - Standards
- Implementation

Biometric System Design

- Enrollment
  - Good enrollment is critical to system performance
  - Operator training, GUI, documentation key
  - Supervised, self-enroll, remote enrollment
  - Who is authorized to enroll/update? Protected function?
  - Capture:
    - Provide visual cues
    - Capture 1 or more biometric types? Demographic data?
    - For each biometric, how many captures needed
      - # fingers, which ones
    - Capture live/electronically or paper/manual (ink on paper)
    - Feedback on possible problems/solutions
      - cold hands/rub together

Enrollment (cont'd)

- Process:
  - Calculate quality and provide feedback to enroller
  - Prompt for recapture if poor quality
  - Process locally or centrally
- Verification check:
  - Test verify after capture to ensure enrolled data is good and matchable
- Storage:
  - Where to store - local, central, smart card
  - Store raw image or just template
  - Data protection - encryption
  - Data synchronization
  - Data back-up/restore, maintenance (deletes)
  - Choice of index

Enrollment (cont'd)

- Updates:
  - Under what conditions will an update be performed?
    - Overt function?
    - Subject initiated?
    - Automatic when better quality data captured?
    - Automatic learn mode?
- Procedures for handling exceptions:
  - Inability to enroll a particular subject
  - Temporarily inaccessible biometric (injury, etc.)
  - Subjects with disabilities
- Quick reference guide
  - Tips on how to get and recognize a good enrollment

Verification

- Capture/process:
  - User interface design
  - May be different than for enrollment
    - Number of captures required
    - Quality feedback
  - Capture trigger (auto/key/timer)
  - Device selection & mounting
  - What do if device broken?
- Verify:
  - Local or central
  - Verify against DB or info on card?
  - If >1 biometric template, try both?
  - Retry mechanism? Any lock-out or alarm conditions?
  - What do for repeated false rejects?

Biometric Algorithms

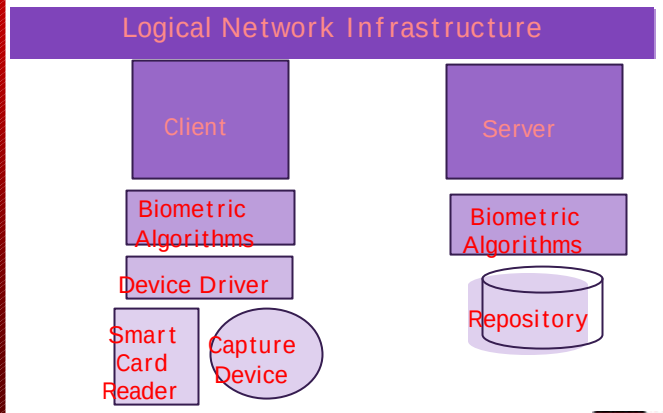
- Proprietary
- Resource requirements
  - Processor speed
  - RAM
  - Data storage
- Platform Requirements
- Hardware acceleration

tuned

Architecture

- The high-level design or the frame that holds the more detailed parts of the design together.
- Qualities
  - Specifies key algorithms and major data structures
  - Allocates functional requirements to components
  - Supports make vs. buy decisions
  - Facilitates project organization
  - Supports a change/growth strategies

Generic Biometric System Architecture



Allocation

- Biometric data storage location
  - Central database
  - Workstation storage
  - Biometric device storage
  - Smart card storage
- Matching location
  - At the central server
  - On the local workstation
  - Within the biometric device
  - On the smart card

•Note: Generally only the biometric template is stored, not the raw data
  –Storage space
  –Transmission bandwidth
  –Privacy concerns
•Processing may be performed at point of capture or point of matching

System Components

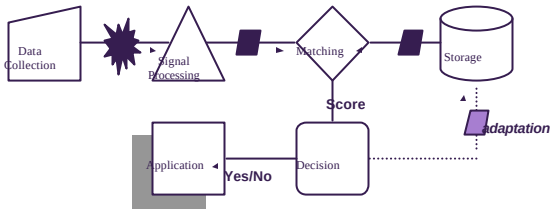
- Network infrastructure
  - Interface: sockets, RPC, CORBA
  - Security
  - Transport
  - Bandwidth
- Repository
  - Algorithm may require proprietary storage
  - Relational database management system (SQL)
  - Directory services
  - Smart card
  - Database synchronization
  - Availability/robustness

Security

- Protection of biometric data
  - Transmission
  - Storage
- Mechanisms
  - Integrity: Digital signatures
  - Privacy: Encryption
  - System Security:
    - Cryptographic techniques, access controls, mutual authentication
    - Use within security architecture (Example: CDSA)
- Guidelines
  - ANSI X984: "Biometric Information Management and Security"
- Considerations
  - Biometrics generally addresses I&A only
  - Consider degree of improvement over current - not just compare to ideal
  - Use in conjunction with other security mechanisms
  - Cost consistent with threat
  - Vulnerabilities
    - Don't add security holes
  - Anti-spoofing mechanisms
  - Trusted client
  - Trusted administrator
    - Enrollment/update/delete privileges
  - Increase cost/sophistication of attack

Security vulnerability points

- ANSI X9.84
  - Protection within components and during transmission



Ancillary Functions

- Analysis:
  - Error/event logs
  - Save failed images?
- Diagnostics:
  - Device checks
  - Remote diagnostics
- Redundancy/failover

Biometric Standards

- Support interoperability and interchangeability
- Reduces risk to integrators and end users
- Biometric Data Standards
  - Common Biometric Exchange File Format (CBEFF) group
    - Defining standard for exchanging biometric data
    - Sponsored by NIST, NSA, and the US Biometric Consortium
    - Supported within ANSI and BioAPI specifications (below)
    - IBIA acting as registration authority for biometric data formats
- Biometric Software Standards
  - BioAPI Consortium - industry consensus open system standard
  - Microsoft - planned incorporation of a proprietary standard
- ANSI subcommittee X9F4 (Financial)
  - Guidelines for use of biometrics to secure transactions
- ISO 7816-11
  - Biometrics and smart cards

Implementation

Solution Alternatives

- "Off the shelf" solution
  - Still limited availability
- Integration of existing components
  - Developer tool kits
  - Customize existing application
  - Open systems architecture for non-biometric components
- Development
  - Avoid NIH syndrome
  - Pushing State of the Art
    - technology or application
  - Require proprietary control

Vendor Selection

- Experience with biometric technology
- Success with similar architecture
- Clear requirements management
- Contract should support
  - Requirements process
  - Milestones with concrete deliverables
  - Change control
  - Test plans and benchmarking
- IBIA membership – standards of:
  - Conduct, ethics, privacy

Capture Hardware Selection

- Dedicated or multi-purpose device
- Self contained (capture, processing, matching, storage)
- Integrated encryption
- Multifunction (include smart card reader, pin pad, mag stripe reader, etc.)
- Embedded in peripheral (keyboard/mouse) or standalone
- Platform Requirements (port type, client rescues, driver support, etc)

Pilot Project

- Common risk management technique
- Need clear objectives for pilot project
- Include measurements to supplement qualitative feedback
  - FAR & FRR
  - Observer users experience
  - Solicit user feedback
- Time and scale based on overall project objectives
- Balance need to market concept with goal to reduce risk

Conclusion

- Biometric integration has some unique considerations
- Match solution to requirements
- Consider exception conditions
- End-to-end system design based on solid, scalable architecture
- Performance keys:
  - Good enrollment
  - Correct threshold setting
- Standards lower risk


Thanks!
For your attention!
13 Sep 2001
(c) SAFLINK 2001
59
saflink